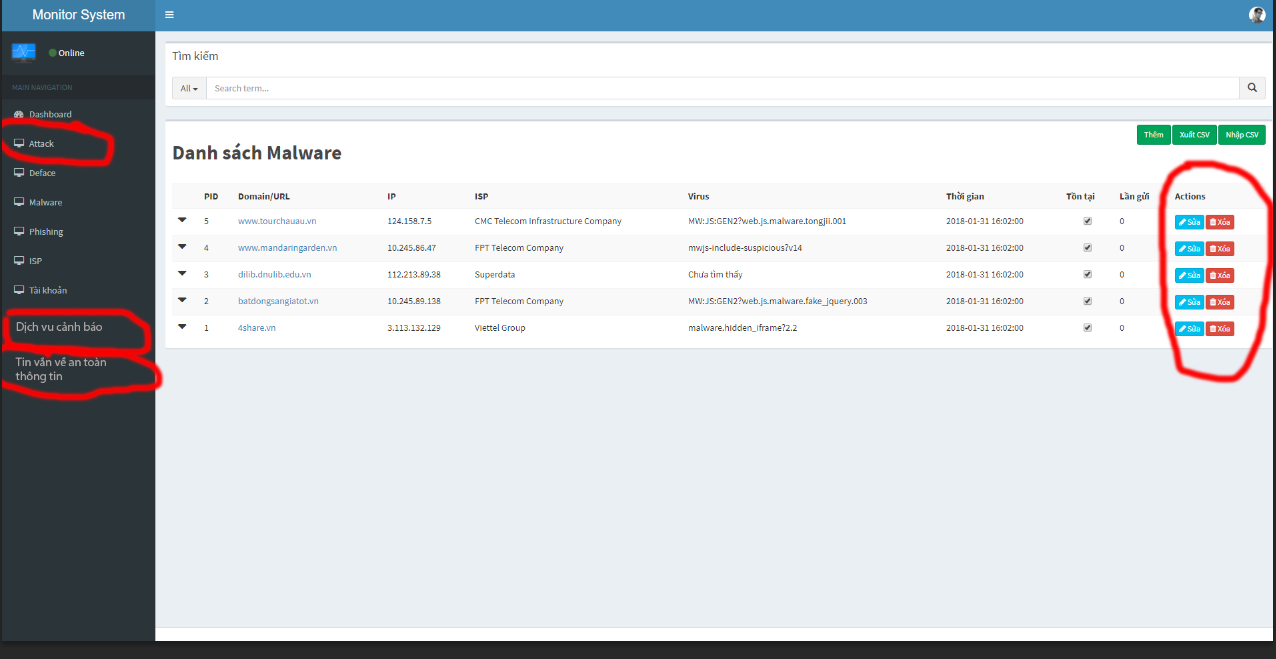
**1, V/v Dữ liệu đẩy lấy trùng lặp:**

Sau khi kiểm tra hệ thống dữ liệu cùng đẩy lên 1 file hai lần, vẫn được thêm hai lần vào database, khi tổng hợp số lượng được tính tổng của hai lần up lên 1 file.

Nếu để lọc trùng thì ảnh hưởng tới hệ thông không cập nhập đầy đủ, vidu sự cố vidu.vn bị malware, phishing … xảy ra 1 ngày, 1 tháng, 1 năm … trước nhưng đến ngày hiện tại bị lại, nếu lọc trùng như cũ sẽ bỏ sót ở hệ thống.

Vậy nên, sẽ check qua Action, nếu sự cố có trùng nhưng action đã được giải quyết rồi, thì sẽ được thêm vào database như một sự cố mới, nếu chưa được sử lý sẽ được thông báo trùng và yêu cầu sử lý hiển thị ra những sự cố trùng.



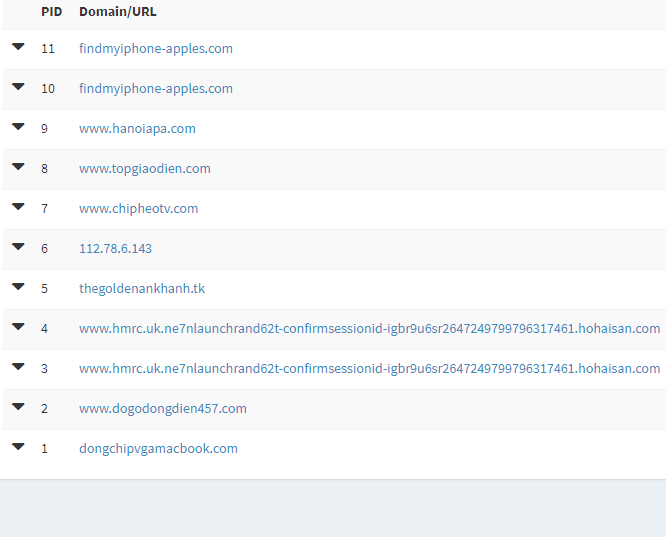
**2. V/v phần mục attack:**

Đẩy các dữ liệu từ file csv được đính kèm theo để bên các bạn phân tích và xây dưng một bảng cho mục attack.

Do cột dữ liệu có thể có thêm, nên linh động trong thêm cột trong database để phù hợp với file.

**3. Gửi email cảnh báo tới đơn vị bị sự cố**

Trong mục malware, deface, phishing



Có thể thấy những dữ liệu trùng lặp domain do sự cố sảy ra ở nhiều đường dẫn khác nhau, ví dụ:

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php

Trường hợp này được coi là một sự cố chứ không phải hai sự cố, vậy nên ở khi hiện thị chỉ cần hiển thị link http[:]//year2000vn.com[.]vn, và có thêm một mũi tên màu xanh đi xuống (để khác với mũi tên đi xuống hiển thị chi tiết) , khi click vào sẽ hiển thị ra các link chi tiết như trên. Các link chi tiết như trên cũng có mũi tên màu đen, ở đầu đường link để click vào xem chi tiết sự cố.

Đầu mỗi sự cố có hiển thị một icon hình email, khi click vào mở ra một cửa sổ mới có mẫu gửi email sẵn:

**Email tiếp nhận:** Lấy từ danh sách mục IPS (linh động có thể sửa được)

**Email CC:** là email để báo cáo (có thể set sẵn vd: [tnchung@vncert.vn](mailto:tnchung@vncert.vn)) hoặc thêm sửa.

**Tiêu đề:** *Đề nghị xử lý sự cố trên dịch vụ của (Tên đơn vị ISP,)*

**Nội dung:**

*Kính gửi (Tên đơn vị ISP,)*

*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, Bộ Thông tin và Truyền thông (VNCERT) ghi nhận, hiện có những domain*

*(Các hoặc một domain bị sự cố vidu nếu click vào email ở đầu đường link*

*http[:]//year2000vn.com[.]vn*

*trong nội hiển thị:*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php*

*)*

*(IP bị sự cố)*

*IP này  thuộc (Tên đơn vị ISP,)  
  
Thực hiện Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, Trung tâm VNCERT đề nghị Quý Công ty xử lý sự cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), và các cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ) trong vòng 24 giờ kể từ khi nhận được Email này nhằm ngăn chặn website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ).  
  
Sau khi hoàn thành việc xóa các website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), đề nghị Công ty gửi báo cáo kết thúc sự cố (ban hành kèm theo Thông tư số 20/2017/TT-BTTTT, có thể tải tại địa chỉ:*[*http://vncert.vn*](http://vncert.vn/)*) về Đầu mối tiếp nhận sự cố của Trung tâm VNCERT qua địa chỉ*[*ir@vncert.vn*](mailto:ir@vncert.vn) *Cảm ơn sự hợp tác của Quý Công ty.*

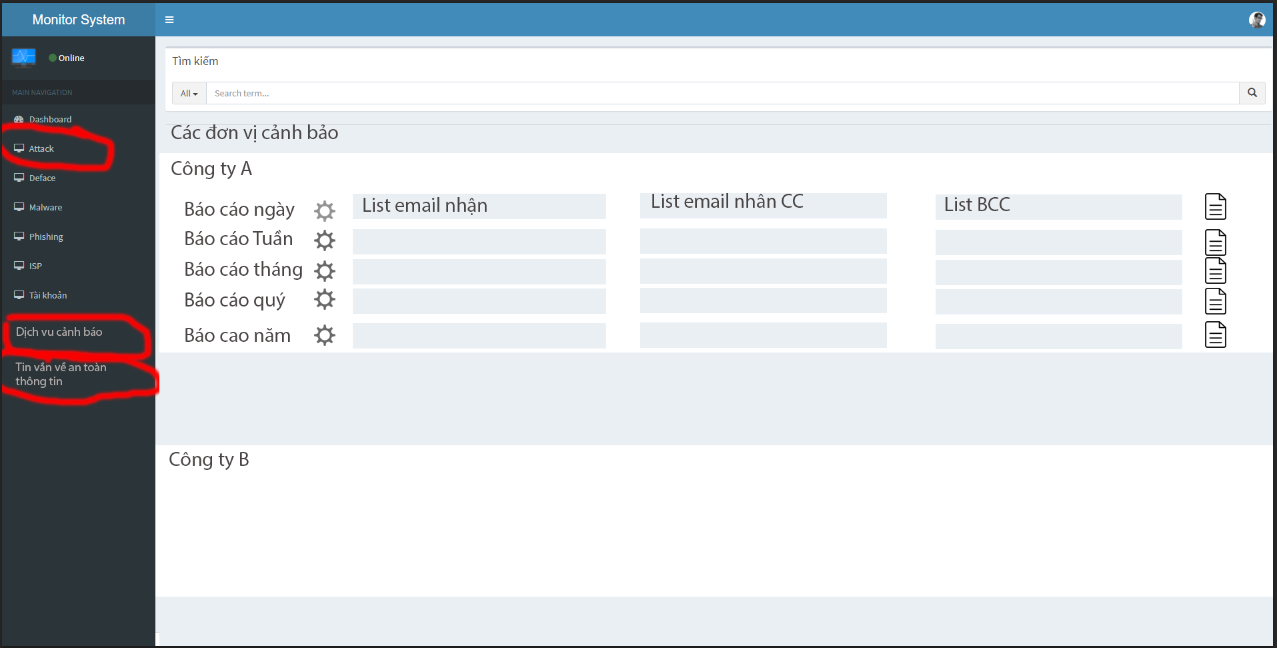
*--------------------------------------------  
Nguyen Thanh Chuong (Mr)  
VNCERT, MIC  
Mobile:*[*+84 91 8228 754*](callto:+84%2091%208228%20754)*Website:*[*www.vncert.gov.vn*](http://www.vncert.gov.vn/)

Tạo Ticket : VNCERT#(Mã số ID của phiếu) lưu nội dung email và thư trả lời từ đơn vị ISP, khi đóng hỗ trợ bên cột Tồn tại cũng được bỏ dấu check.

Thêm một mục trên menu, Hỗ trợ sử lý sự cố hoặc sử lý sự cố, khu vực này có thể nhận dc email trả lời cũng như trả lời lại ISP và đóng phiếu hỗ trợ.

**4. Phần “Dịch vụ cảnh báo”:**

Giao diện:



Click vào icon setting để cài đặt ngày giờ tự động gửi đi theo GMT +7.

Click vào icon document để xem các file gửi đi (số lượng file gửi đi giữa các ngày, tuần, quý … khác nhau), và mẫu tempalte gửi đi, có thể sửa lại các mẫu template với các tham số được lấy từ “Mục tin vắn trong ngày” “deface,malware, phishing” .

**Hoạt động**

Cơ quan cung các giải ip dải ip (theo AS hoặc theo IP), hệ thông so sánh giải ip với các ip thuộc sự cố trong ngày (trong mục attack, malware, phishing,deface) thông kê nếu có ip trùng thì báo cáo sự cố theo mẫu dưới và kèm theo file đính kèm thông báo chi tiết sự cố:

**Mẫu báo cáo ngày (BCN):**

|  |
| --- |
| Kính gửi đầu mối tiếp nhận sự cố XXX,  Trong quá trình theo dõi sự cố tại Việt Nam, Trung tâm VNCERT phát hiện các sự cố liên quan đến XXXX.  Danh sách các sự cố được gửi trong tập tin đính kèm (nếu có, nếu không có sẽ không có file đính kèm).  Trân trọng./. |

Nếu không có sự cố nào xảy ra thì gửi email theo mẫu trên và không có file đính kèm theo email.

File đính kèm có dạng yyyymmdd\_XXX\_Report.pdf

Nội dung báo cáo gửi đính kèm theo email:

|  |
| --- |
| C:\Users\nguye\AppData\Local\Microsoft\Windows\INetCache\Content.Word\20180130_xxx_Report.png |

**Báo cáo tháng (BCT):**

Bao gồm 1 file như mẫu báo cáo ngày (BCN) list ra các sự cố trong tuần.

Một file về thông tin an toàn thông tin của tuần: “Thong tin ATTT tuan x thang x nam x.pdf”

Nội dung: